IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.*

Examiner: Pyzocha, Michael J.

Serial No.: 09/919,248

Group Art Unit: 2137

Filed: 07/31/2001

DOCKET NO.: **RSW920010143US1**

Title: **AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

This Appeal Brief, pursuant to the Notice of Appeal filed July 3, 2006, is an appeal from the rejection of the Examiner in the Office Action dated April 3, 2006.

REAL PARTY IN INTEREST

International Business Machines, Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 3-11 and 13-20 are rejected. Claims 1, 2 and 12 are canceled. This Brief is in support of an appeal from the rejection of claims 3-11 and 13-20.

STATUS OF AMENDMENTS

There are no After-Final Amendments which have not been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 3 - INDEPENDENT

The present invention provides an authentication method for electronic mail (see specification, page 2, lines 11-14; page 4, lines 7-10). An authentication key associated with an originator (100 in FIG. 1) is stored in a memory (130 in FIG. 1) of the originator (see specification, page 6, lines 18-19). The authentication key is read from the memory of the originator; electronic mail is prepared for sending from the originator to a recipient such that the authentication key, that had been read from the memory of the originator, is included in an open field of the electronic mail (see steps 205 and 210 in FIG. 2; specification, page 7, lines 4-7, 12-15). The electronic mail is sent from the originator to the recipient (see step 215 in FIG. 2; specification, page 7, lines 16-17).

B. CLAIM 6 - INDEPENDENT

The present invention provides an authentication method for electronic mail (see specification, page 2, lines 11-14; page 4, lines 7-10). An authentication key is stored in a memory (180 in FIG. 1) of a recipient (150 in FIG. 1) of the electronic mail at an address that is dependent upon a source identifier that identifies an originator (100 in FIG. 1) of the electronic mail (see specification, page 6, lines 18-20; page 8, lines 16-20). The recipient receives the electronic mail from the originator (see step 220 in FIG. 2; specification, page 7, lines 16-17).

Responsive to receiving the electronic mail, it is determined whether the authentication key is present in an open field of the electronic mail (see step 235 in FIG. 2; specification, page 8, lines 8-10). Responsive to determining that the authentication key is present, it is determined whether the authentication key is associated with the originator (see step 245 in FIG. 2; specification, page 8, lines 13-15). Responsive to determining that the authentication key is not associated with the originator, the electronic mail is rejected (see step 240 in FIG. 2; specification, page 9, lines 3-4). Said determining whether the authentication key is associated with the originator includes: reading the stored authentication key from the address at the memory of the recipient, and comparing the authentication key with the stored authentication key that had been read from the address at the memory of the recipient to determine whether the authentication key is associated with the originator (see specification, page 8, lines 16-20).

C. CLAIM 8 - INDEPENDENT

The present invention provides an authentication method for electronic mail (see specification, page 2, lines 11-14; page 4, lines 7-10). A recipient (150 in FIG. 1) receives electronic mail from an originator (100 in FIG. 1) (see step 220 in FIG. 2; specification, page 7, lines 16-17). Responsive to receiving the electronic mail, it is determined whether the authentication key is expected to be present in an open field of the electronic mail (see step 225 in FIG. 2; specification, page 7, lines 18 - page 8, line 1). Responsive to determining that the authentication key is expected to be present, it is determined whether the authentication key is present (see step 235 in FIG. 2; specification, page 8, lines 8-10). Responsive to determining that the authentication key is not expected to be present, the electronic mail is accepted (see step 230

in FIG. 2; specification, page 8, lines 3-4).

D. CLAIM 9 - INDEPENDENT

The present invention provides an authentication method for electronic mail (see specification, page 2, lines 11-14; page 4, lines 7-10). A recipient (150 in FIG. 1) receives electronic mail from an originator (100 in FIG. 1) (see step 220 in FIG. 2; specification, page 7, lines 16-17). Responsive to receiving the electronic mail, it is determined whether the authentication key is expected to be present in an open field of the electronic mail (see step 225 in FIG. 2; specification, page 7, lines 18 - page 8, line 1). Responsive to determining that the authentication key is expected to be present, it is determined whether the authentication key is present (see step 235 in FIG. 2; specification, page 8, lines 8-10). Responsive to determining that the authentication key is not present, the electronic mail is rejected (see step 240 in FIG. 2; specification, page 8, lines 10-11). Responsive to determining that the authentication key is present, it is determined whether the authentication key is associated with the originator (see step 245 in FIG. 2; specification, page 8, lines 13-15). Responsive to determining that the authentication key is associated with the originator, the electronic mail is accepted (see step 230 in FIG. 2; specification, page 9, lines 1-3). Responsive to determining that the authentication key is not associated with the originator, the electronic mail is rejected (see step 240 in FIG. 2; specification, page 9, lines 3-4).

E. CLAIM 13 - INDEPENDENT

The present invention provides an authentication method for electronic mail (see

specification, page 2, lines 11-14; page 4, lines 7-10). A recipient (150 in FIG. 1) receives electronic mail from an originator (100 in FIG. 1) (see step 220 in FIG. 2; specification, page 7, lines 16-17). The electronic mail havd been previously prepared for sending from the originator to the recipient (see step 205 in FIG. 2; specification, page 7, lines 4-6). Responsive to receiving the electronic mail, it is determined whether the authentication key is expected to be present in an open field of the electronic mail (see step 225 in FIG. 2; specification, page 7, lines 18 - page 8, line 1). Responsive to determining that the authentication key is expected to be present, it is determined whether the authentication key is present (see step 235 in FIG. 2; specification, page 8, lines 8-10). Responsive to determining that the authentication key is not present in the open field of the electronic mail, the electronic mail is rejected (see step 240 in FIG. 2; specification, page 8, lines 10-11).

F. CLAIM 14 - INDEPENDENT

The present invention provides an authentication method for electronic mail having a subject line (see specification, page 2, lines 11-14; page 4, lines 7-10; page 9, lines 5-8). A recipient (150 in FIG. 1) receives electronic mail from an originator (100 in FIG. 1) (see step 220 in FIG. 2; specification, page 7, lines 16-17). The electronic mail havd been previously prepared for sending from the originator with a source identifier to the recipient with a destination identifier (see step 205 in FIG. 2; specification, page 7, lines 4-6; page 3, lines 4-5; page 7, lines 10-12). Responsive to receiving the electronic mail, it is determined whether the authentication key is expected to be present in an open field of the electronic mail (see step 225 in FIG. 2; specification, page 7, lines 18 - page 8, line 1). Responsive to determining that the authentication

key is not expected to be present, the electronic mail is accepted (see step 230 in FIG. 2; specification, page 8, lines 3-4). Responsive to determining that the authentication key is expected to be present, it is determined whether the authentication key is present (see step 235 in FIG. 2; specification, page 8, lines 8-10). Responsive to determining that the authentication key is present, it is determined whether the authentication key is associated with both the originator and the receipient (see step 245 in FIG. 2; specification, page 8, lines 13-17). Responsive to determining that the authentication key is not associated with both the originator and the receipient, the electronic mail is rejected (see step 240 in FIG. 2; specification, page 9, lines 3-4). Responsive to determining that the authentication key is not present, the electronic mail is rejected (see step 240 in FIG. 2; specification, page 8, lines 10-11).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 8-9, 13-14 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Lindeman *et al.* (US 2003/0009698).

2. Claims 3-5, 15, 17-18 and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Lindeman in view of Leeds (US 2002/0016824).

3. Claims 6-7, 10-11, 16 and 19 stand rejejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over the modified Lindeman and Leeds system and further in view of Liu *et al.* (US 6,760,752).

ARGUMENT

GROUND OF REJECTION 1

Claims 8-9, 13-14 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Lindeman *et al.* (US 2003/0009698).

Claim 8

Appellants respectfully contend that Lindeman does not anticipate claim 8, because Lindeman does not teach each and every feature of claim 8.

As a first example of why Lindeman does not anticipate claim 8, Lindeman does not teach the feature: "responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail; responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present".

In the Advisory Action mailed 06/09/2006, the Examiner argues: "With respect to Applicant's argument that Lindeman fails to disclose determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password, the system expects the CZID to be present and in paragraph 106 lines 7-9 Lindeman discloses the CZID being in an open field of the electronic mail, specifically the subject. Furthermore, Lindeman discloses in response to determining the key is expected to be present, determining if it is present, as exemplified above, when there is no tunnel password the CZID is expected to be

present and there is a determination as to whether it is present."

Appellants maintain that the preceding argument by the Examiner fails to recognize that the preceding feature of claim 8 includes two distinctive tests, namely a first test of whether an authentication key is expected to be present in an open field of the electronic mail, and a second test (responsive to determining that the authentication key is expected to be present) of whether the authentication key is present. The preceding two distinctive tests are shown as distinctive steps 225 and 235 in FIG. 2 of Appellants' patent application.

In contrast and noting that the Examiner alleges that the CZID in Lindeman represents the claimed authentication key, the flow chart of Sheet 7 of Lindeman does not depict any test of whether the CZID is expected to be present in an open field of the electronic mail and depicts only the test in step 708 of whether the CZID is present. The Examiner's allegation that Lindeman "disclose[s] determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password" is incorrect. It is clear from the flow chart of Sheet 7 of Lindeman that if in step 704 it is determined that there is no tunnel password, then step 708 is next performed to determine whether the CZID is present. No test is ever made in Lindeman of whether the CZID is expected to be present.

Therefore, Lindeman does not teach the preceding feature of claim 8.

As a second example of why Lindeman does not anticipate claim 8, Lindeman does not teach the feature: "responsive to determining that the authentication key is not expected to be present, accepting the electronic mail".

One reason why Lindeman does not teach the preceding feature of claim 8 is that Lindeman does not teach determining that the authentication key is not expected to be present, as explained *supra*.

In addition, in the Advisory Action mailed 06/09/2006, the Examiner argues: "Lindeman discloses accepting the email when determining that the key is not expected to be present, when the CZID is not present the message is checked to determine if it is from a trusted sender, group or domain, and if it is then a CZID is not expected and the message is accepted. These steps are exemplified in figure 7 and the corresponding description in the specification."

Appellants maintain that the preceding argument by the Examiner is based on an incorrect analysis of the flow chart of Sheet 7 of Lindeman and the accompanying description. In particular, Lindeman does not teach that a CZID is not expected to be present if the CZID is determined in step 708 to not be present and if the message is determined in step 716 to have been sent from a trusted sender.

Therefore, Lindeman does not teach the preceding feature of claim 8.

Based on the preceding arguments, Appellants respectfully maintain that Lindeman does not anticipate claim 8, and that claim 8 is in condition for allowance.

Claim 9

Appellants respectfully contend that Lindeman does not anticipate claim 9, because Lindeman does not teach each and every feature of claim 9.

As a first example of why Lindeman does not anticipate claim 9, Lindeman does not teach the feature: "responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail; responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present".

In the Advisory Action mailed 06/09/2006, the Examiner argues: "With respect to Applicant's argument that Lindeman fails to disclose determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password, the system expects the CZID to be present and in paragraph 106 lines 7-9 Lindeman discloses the CZID being in an open field of the electronic mail, specifically the subject. Furthermore, Lindeman discloses in response to determining the key is expected to be present, determining if it is present, as exemplified above, when there is no tunnel password the CZID is expected to be present and there is a determination as to whether it is present."

Appellants maintain that the preceding argument by the Examiner fails to recognize that the preceding feature of claim 9 includes two distinctive tests, namely a first test of whether an authentication key is expected to be present in an open field of the electronic mail, and a second test (responsive to determining that the authentication key is expected to be present) of whether the authentication key is present. The preceding two distinctive tests are shown as distinctive steps 225 and 235 in FIG. 2 of Appellants' patent application.

In contrast and noting that the Examiner alleges that the CZID in Lindeman represents the claimed authentication key, the flow chart of Sheet 7 of Lindeman does not depict any test of

whether the CZID is expected to be present in an open field of the electronic mail and depicts only the test in step 708 of whether the CZID is present. The Examiner's allegation that Lindeman "disclose[s] determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password" is incorrect. It is clear from the flow chart of Sheet 7 of Lindeman that if in step 704 it is determined that there is no tunnel password, then step 708 is next performed to determine whether the CZID is present. No test is ever made in Lindeman of whether the CZID is expected to be present.

Therefore, Lindeman does not teach the preceding feature of claim 9.

As a second example of why Lindeman does not anticipate claim 9, Lindeman does not teach the feature: "responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present; responsive to determining that the authentication key is not present, rejecting the electronic mail".

One reason why Lindeman does not teach the preceding feature of claim 9 is that Lindeman does not teach determining that the authentication key is expected to be present, as explained *supra*.

In addition, Appellants maintain that determining that the authentication key is expected to be present and determining that the authentication key is not present are **sufficient conditions** for rejecting the electronic mail, as illustrated in the execution of rejection step 240 following a "Yes" response to the "Key Expected" decision block and a "No" response to the "Key Present" decision block in Appellants' FIG. 2.

In contrast, a determination in step 708 in the flow chart of Sheet 7 of Lindeman that the

CZID is not present is **not a sufficient condition** for rejecting the electronic mail. For example, if step 708 determines that the CZID is not present and step 716 determines that the sender is not a trusted sender and step 724 determines that the sender or recipient address is not blacklisted , then the electronic mail is not rejected but rather is accepted in step 736.

Therefore, Lindeman does not teach the preceding feature of claim 9.

Based on the preceding arguments, Appellants respectfully maintain that Lindeman does not anticipate claim 9, and that claim 9 is in condition for allowance.

Claim 13

Appellants respectfully contend that Lindeman does not anticipate claim 13, because Lindeman does not teach each and every feature of claim 13.

As a first example of why Lindeman does not anticipate claim 13, Lindeman does not teach the feature: "responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail; responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present".

In the Advisory Action mailed 06/09/2006, the Examiner argues: "With respect to Applicant's argument that Lindeman fails to disclose determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password, the system expects the CZID to be present and in paragraph 106 lines 7-9 Lindeman discloses the

CZID being in an open field of the electronic mail, specifically the subject. Furthermore, Lindeman discloses in response to determining the key is expected to be present, determining if it is present, as exemplified above, when there is no tunnel password the CZID is expected to be present and there is a determination as to whether it is present."

Appellants maintain that the preceding argument by the Examiner fails to recognize that the preceding feature of claim 13 includes two distinctive tests, namely a first test of whether an authentication key is expected to be present in an open field of the electronic mail, and a second test (responsive to determining that the authentication key is expected to be present) of whether the authentication key is present. The preceding two distinctive tests are shown as distinctive steps 225 and 235 in FIG. 2 of Appellants' patent application.

In contrast and noting that the Examiner alleges that the CZID in Lindeman represents the claimed authentication key, the flow chart of Sheet 7 of Lindeman does not depict any test of whether the CZID is expected to be present in an open field of the electronic mail and depicts only the test in step 708 of whether the CZID is present. The Examiner's allegation that Lindeman "disclose[s] determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password" is incorrect. It is clear from the flow chart of Sheet 7 of Lindeman that if in step 704 it is determined that there is no tunnel password, then step 708 is next performed to determine whether the CZID is present. No test is ever made in Lindeman of whether the CZID is expected to be present.

Therefore, Lindeman does not teach the preceding feature of claim 13.

As a second example of why does not anticipate claim 13, Lindeman does not teach the

feature: "responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present; responsive to determining that the authentication key is not present in the open field of the electronic mail, rejecting the electronic mail".

One reason why Lindeman does not teach the preceding feature of claim 13 is that Lindeman does not teach determining that the authentication key is expected to be present, as explained *supra*.

In addition, Appellants maintain that determining that the authentication key is expected to be present and determining that the authentication key is not present are **sufficient conditions** for rejecting the electronic mail, as illustrated in the execution of rejection step 240 following a "Yes" response to the "Key Expected" decision block and a "No" response to the "Key Present" decision block in Appellants' FIG. 2.

In contrast, a determination in step 708 in the flow chart of Sheet 7 of Lindeman that the CZID is not present is **not a sufficient condition** for rejecting the electronic mail. For example, if step 708 determines that the CZID is not present and step 716 determines that the sender is not a trusted sender and step 724 determines that the sender or recipient address is not blacklisted , then the electronic mail is not rejected but rather is accepted in step 736.

Therefore, Lindeman does not teach the preceding feature of claim 13.

Based on the preceding arguments, Appellants respectfully maintain that Lindeman does not anticipate claim 13, and that claim 13 is in condition for allowance.

Claim 14

Appellants respectfully contend that Lindeman does not anticipate claim 14, because Lindeman does not teach each and every feature of claim 14.

As a first example of why Lindeman does not anticipate claim 14, Lindeman does not teach the feature: "responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail; ... responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present".

the authentication key is expected to be present) of whether the authentication key is present

In the Advisory Action mailed 06/09/2006, the Examiner argues: "With respect to Applicant's argument that Lindeman fails to disclose determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password, the system expects the CZID to be present and in paragraph 106 lines 7-9 Lindeman discloses the CZID being in an open field of the electronic mail, specifically the subject. Furthermore, Lindeman discloses in response to determining the key is expected to be present, determining if it is present, as exemplified above, when there is no tunnel password the CZID is expected to be present and there is a determination as to whether it is present."

Appellants maintain that the preceding argument by the Examiner fails to recognize that the preceding feature of claim 14 includes two distinctive tests, namely a first test of whether an authentication key is expected to be present in an open field of the electronic mail, and a second test (responsive to determining that the authentication key is expected to be present) of whether

the authentication key is present. The preceding two distinctive tests are shown as distinctive steps 225 and 235 in FIG. 2 of Appellants' patent application.

In contrast and noting that the Examiner alleges that the CZID in Lindeman represents the claimed authentication key, the flow chart of Sheet 7 of Lindeman does not depict any test of whether the CZID is expected to be present in an open field of the electronic mail and depicts only the test in step 708 of whether the CZID is present. The Examiner's allegation that Lindeman "disclose[s] determining whether an authentication key is expected to be present in an open field of an email, whenever there is no tunnel password" is incorrect. It is clear from the flow chart of Sheet 7 of Lindeman that if in step 704 it is determined that there is no tunnel password, then step 708 is next performed to determine whether the CZID is present. No test is ever made in Lindeman of whether the CZID is expected to be present.

Therefore, Lindeman does not teach the preceding feature of claim 14.

As a second example of why Lindeman does not anticipate claim 14, Lindeman does not teach the feature: "responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present; ... responsive to determining that the authentication key is not present, rejecting the electronic mail".

One reason why Lindeman does not teach the preceding feature of claim 14 is that Lindeman does not teach determining that the authentication key is expected to be present, as explained *supra*.

In addition, Appellants maintain that determining that the authentication key is expected to be present and determining that the authentication key is not present are **sufficient conditions**

for rejecting the electronic mail, as illustrated in the execution of rejection step 240 following a "Yes" response to the "Key Expected" decision block and a "No" response to the "Key Present" decision block in Appellants' FIG. 2.

In contrast, a determination in step 708 in the flow chart of Sheet 7 of Lindeman that the CZID is not present is **not a sufficient condition** for rejecting the electronic mail. For example, if step 708 determines that the CZID is not present and step 716 determines that the sender is not a trusted sender and step 724 determines that the sender or recipient address is not blacklisted , then the electronic mail is not rejected but rather is accepted in step 736.

Therefore, Lindeman does not teach the preceding feature of claim 14.

As a third example of why Lindeman does not anticipate claim 14, Lindeman does not teach the feature: "responsive to determining that the authentication key is not expected to be present, accepting the electronic mail".

One reason why Lindeman does not teach the preceding feature of claim 14 is that Lindeman does not teach determining that the authentication key is not expected to be present, as explained *supra*.

In addition, in the Advisory Action mailed 06/09/2006, the Examiner argues: "Lindeman discloses accepting the email when determining that the key is not expected to be present, when the CZID is not present the message is checked to determine if it is from a trusted sender, group or domain, and if it is then a CZID is not expected and the message is accepted. These steps are exemplified in figure 7 and the corresponding description in the specification."

Appellants maintain that the preceding argument by the Examiner is based on an incorrect

analysis of the flow chart of Sheet 7 of Lindeman and the accompanying description. In particular, Lindeman does not teach that a CZID is not expected to be presentand if the message is determined in step 716 to have been sent from a trusted sender.

Therefore, Lindeman does not teach the preceding feature of claim 14.

As a fourth example of why Lindeman does not anticipate claim 14, Lindeman does not teach the feature: "responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present; responsive to determining that the authentication key is present, determining whether the authentication key is associated with both the originator and the recipient; responsive to determining that the authentication key is associated with both the originator and the recipient, accepting the electronic mail".

One reason why Lindeman does not teach the preceding feature of claim 14 is that Lindeman does not teach determining that the authentication key is not expected to be present, as explained *supra*.

In addition, the Examiner alleges that the preceding feature of claim 14 is disclosed in Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7, but provides no analysis to demonstrate that the preceding feature of claim 14 is disclosed in Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7. Appellant maintains that the preceding feature of claim 14 is not disclosed in Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7. For example, Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7 does not teach "determining whether the authentication key is associated with both the originator and the recipient". As another example, Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7 does not teach "responsive to determining that the authentication key is associated with both the

originator and the recipient, accepting the electronic mail".

Therefore, Lindeman does not teach the preceding feature of claim 14.

As a fifth example of why Lindeman does not anticipate claim 14, Lindeman does not teach the feature: "responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present; responsive to determining that the authentication key is present, determining whether the authentication key is associated with both the originator and the recipient; ... responsive to determining that the authentication key is not associated with both the originator and the recipient, rejecting the electronic mail".

One reason why Lindeman does not teach the preceding feature of claim 14 is that Lindeman does not teach determining that the authentication key is not expected to be present, as explained *supra*.

In addition, the Examiner alleges that the preceding feature of claim 14 is disclosed in Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7, but provides no analysis to demonstrate that the preceding feature of claim 14 is disclosed in Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7. Appellant maintains that the preceding feature of claim 14 is not disclosed in Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7. For example, Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7 does not teach "determining whether the authentication key is associated with both the originator and the recipient". As another example, Lindeman, Pars. 83-84, 103-106 and FIGS. 5-7 does not teach "responsive to determining that the authentication key is not associated with both the originator and the recipient, rejecting the electronic mail".

Therefore, Lindeman does not teach the preceding feature of claim 14.

Based on the preceding arguments, Appellants respectfully maintain that Lindeman does not anticipate claim 14, and that claim 14 is in condition for allowance.

GROUND OF REJECTION 2

Claims 3-5, 15, 17-18 and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Lindeman in view of Leeds (US 2002/0016824).

Claims 3-5 and 15

Appellants respectfully contend that claim 3 is not unpatentable over Lindeman in view of Leeds, because Lindeman in view of Leeds does not teach or suggest each and every feature of claim 3.

As a first example of why claim 3 is not unpatentable over Lindeman in view of Leeds, Appellants maintain that Lindeman in view of Leeds does not teach or suggest the feature: "storing an authentication key associated with an originator in a memory of the originator; reading the authentication key from the memory of the originator; preparing electronic mail for sending from the originator to a recipient, said preparing comprising including the authentication key, that had been read from the memory of the originator, in an open field of the electronic mail".

In the Advisory Action mailed 06/09/2006, the Examiner argues: "With respect to Applicant's argument that Leeds fails to teach storing an authentication key associated with an originator, this limitation is clearly disclosed in paragraph 37 lines 12-21. "

Appellant note that Leeds, Par. 37, lines 12-21 recites: "That is, when a message is received, the mail program or mail handling system would send the unique code and the "From:" identifier to the authenticator for authentication. The code and the "From:" identifier would be checked against the database of known junk e-mailers as well as checked for consistency

between the two parts. If the code was for a known junk e-mailer, or if the code and the "From:" field did not match, the mail program or mail handling system would be warned of the problem" (emphasis added).

Thus, what is stored in the database is not "an authentication key associated with an originator" as is required by claim 3, but rather is known junk e-mailers. Thus Leeds does not disclose the preceding feature of claim 3.

Moreover, even if one of the stored junk e-mailers is "an authentication key associated with an originator", Leeds does not teach that the junk e-mailer authentication key is "stored in a memory of the originator" as is required by claim 3. Appellant notes from Leeds, Pars. 36-37 that the database of known junk e-mailers is in a memory of the authenticator and not in a memory of the originator. Thus Leeds does not disclose the preceding feature of claim 3.

Moreover, even if one of the stored junk e-mailers is "an authentication key associated with an originator", Leeds does not disclose reading the junk e-mailer authentication key from the memory of the originator and including the junk e-mailer authentication key, **that had allegedly been read from the memory of the originator**, in an open field of the electronic mail, as is required by claim 3. Thus Leeds does not disclose the preceding feature of claim 3.

In further response, respectfully contend that the Examiner's argument for incorporating the alleged teaching of Leeds into the system of Lindeman is not persuasive.

The Examiner argues: "At the time of the invention it would have been obvious to a person of ordinary skill in the art to store and read the authentication key of Lindeman from memory.... Motivation to do so would have been to determine when email is junk email (see

paragraph 36)."

In response, Appellants assert that Leeds, Paragraph 36 does not teach that the determination of when email is junk email is facilitated by performance of "storing an authentication key associated with an originator in a memory of the originator; reading the authentication key from the memory of the originator". Rather, Leeds, Paragraph 36 teaches that "the authenticator would potentially be receiving additional information on whether or not a message was a junk e-mail while the message was present in a user's inbox", which is how Lindeman determines when email is junk email.

Moreover, Leeds does not offer any reason as to why it is obvious to store and read the authentication key **in a memory of the originator**. Leeds teaches away from storing and reading the authentication key in a memory of the originator, by stating that the database of junk e-mailers is stored in a memory of the authenticator.

Based on the preceding argument, Appellants respectfully contend that claim 3 is not unpatentable over Lindeman in view of Leeds and is in condition for allowance. Since claims 4-5 and 15 depend from claim 3, Appellants contend that claims 4-5 and 15 are likewise in condition for allowance.

In addition with respect to claim 15, Appellants respectfully contend that Lindeman in view of Leeds does not teach or suggest the feature: "wherein the authentication key is dependent upon only an identity of the originator".

The Examiner argues: "the modified Lindeman and Leeds system discloses the authentication key is dependent upon only an identity of the originator (see Leeds paragraphs 36

and 37) ."

In response, Appellants maintain that the Examiner has not provided motivation from the prior art for modifying Lindeman with the alleged teaching of Leads with respect to the feature: "wherein the authentication key is dependent upon only an identity of the originator".

In addition, any such modification of Lindeman would destroy the teaching of the CZID of Lindeman, wherein the CZID is essential to Lindeman's invention. See Lindeman, Paragraph 29 (" The CZID is **necessary** to authenticate the confirmation message" (emphasis added)). Moreover, the CZID is not dependent upon only an identity of the originator. See Lindeman, Paragraph 31("The term "CZID" is an MD5 hash of the original sender address, the original destination address, and a secret string. A valid CZID is used to authenticate a message, the source email address, and the destination email address to Spam filter" (emphasis added)). Therefore, the Examiner's suggested modification of Lindeman would destroy Lindeman's invention.

Based on the preceding argument, Appellants respectfully contend that claim 15 is not unpatentable over Lindeman in view of Leeds.

Claims 17-18 and 20

Since claims 17, 18, and 20 depend respectively from claims 8, 9, and 13, which Appellants have argued *supra* to not be unpatentable over Lindeman under 35 U.S.C. §102(e), Appellants maintain that claims 17, 18, and 20 are likewise not unpatentable over Lindeman in view of Leeds under 35 U.S.C. §103(a).

In addition, with respect to claims 17, 18, and 20, Appellants respectfully contend that Lindeman in view of Leeds does not teach or suggest the feature: "wherein the authentication key is dependent upon only an identity of the originator".

The Examiner argues: "the modified Lindeman and Leeds system discloses the authentication key is dependent upon only an identity of the originator (see Leeds paragraphs 36 and 37) ."

In response, Appellants maintain that the Examiner has not provided motivation from the prior art for modifying Lindeman with the alleged teaching of Leads with respect to the feature: "wherein the authentication key is dependent upon only an identity of the originator".

In addition, any such modification of Lindeman would destroy the teaching of the CZID of Lindeman, wherein the CZID is essential to Lindeman's invention. See Lindeman, Paragraph 29 (" The CZID is **necessary** to authenticate the confirmation message" (emphasis added)). Moreover, the CZID is not dependent upon only an identity of the originator. See Lindeman, Paragraph 31("The term "CZID" is an MD5 hash of the original sender address, the original destination address, and a secret string. A valid CZID is used to authenticate a message, the source email address, and the destination email address to Spam filter" (emphasis added)). Therefore, the Examiner's suggested modification of Lindeman would destroy Lindeman's invention.

Based on the preceding argument, Appellants respectfully contend that claims 17, 18, and 20 are not unpatentable over Lindeman in view of Leeds.

GROUND OF REJECTION 3

Claims 6-7, 10-11, 16 and 19 stand rejejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over the modified Lindeman and Leeds system and further in view of Liu *et al.* (US 6,760,752).

Claims 6-7 and 16

Appellants respectfully contend that claim 6 is not unpatentable over Lindeman and Leeds in further view of Liu, because Lindeman and Leeds in further view of Liu does not teach or suggest each and every feature of claim 6.

As a first example of why claim 6 is not unpatentable over Lindeman and Leeds in further view of Liu, Lindeman in view of Leeds does not teach or suggest the feature: "storing an authentication key **in a memory of a recipient of the electronic mail** at an address that is dependent upon a source identifier that identifies an originator of the electronic mail" (emphasis added).

The Examiner argues: "The modified Lindeman and Leeds system fails to disclose the address at which the key is stored is dependent upon a source identifier that identifies the originator. However, Liu et al teaches such addressing (see column 19 line 57 through column 20 line 14)."

In the Advisory Action mailed 06/09/2006, the Examiner further argues: "With respect to Applicant's argument that Liu et al fails to disclose storing an authentication key in a memory of a recipient of the electronic mail at an address that is dependent upon a source identifier that identifies an originator of the email, Liu teaches storing a key in a memory dependent upon a

source identifier that identifies an originator of the email in column 20 lines 6-14."

In response, Appellants contend that Liu, col. 19, line 57 - col. 20, line 14 does not disclose that anything is stored in a memory of a recipient of the electronic mail. The Examiner arrears to be relying on Liu, col. 20, lines 5-8 which recites: "The status of the recovery data is maintained along with the recovery data in a recovery database. In one implementation, the recovery database is indexed by the owner's E-mail address or the hash of the E-mail address." Appellants note, however, that Liu does not disclose that the recovery database is in a memory of a recipient of the electronic mail, as required by claim 6. In fact, Liu, col. 19, line 57 - col. 20, line 14 describes steps performed by key server 108 of FIG. 1. Appellants note from Liu, FIG. 1 that the key server 108 is distinct from the recipient 104 and is separated from the recipient 104 by an internet network 106. Therefore, the recover database discussed in Liu, col. 20, lines 5-8 is most likely in a memory of the key server 108 rather than in a memory of the recipient 104. Therefore, the Examiner's argument that Liu, col. 19, line 57 - col. 20, line 14 teaches the preceding feature of claim 6 is incorrect.

In addition, Appellants respectfully contend that the Examiner's argument for modifying Lindeman with the alleged teaching of Liu is not persuasive. The Examiner argues: "At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the authentication key of the modified Lindeman and Leeds system in an address dependent upon a source identifier of the originator.... Motivation to do so would have been store the information in a recovery database (see Liu et al column 19 line 57 through column 20 line 14)."

In response, Appellants assert that the Examiner's stated reason for modifying Liu does not have any relationship to Lindeman's invention and is therefore not an obvious modification

of Lindeman. In particular, the Examiner has not provided any reason why Lindeman's invention would benefit from storing "the information" in a recovery database located in the memory oif the recipient. Accordingly, the Examiner has not established a *prima facie* case of obviousness in relation to claim 6.

As a second example of why claim 6 is not unpatentable over Lindeman and Leeds in further view of Liu, Lindeman in view of Leeds does not teach or suggest the feature: "wherein said determining whether the authentication key is associated with the originator includes: reading the stored authentication key from the address at the memory of the recipient, and comparing the authentication key with the stored authentication key that had been read from the address at the memory of the recipient to determine whether the authentication key is associated with the originator".

The Examiner alleges that the preceding feature is disclosed in Lindeman, Paragraphs 83-84, 102-103, and 36-37.

In response, Appellants maintain that Lindeman does not disclose said "reading" and furthermore does not disclose said "comparing". The Examiner has not provided analysis to support the Examiner's allegation that Lindeman, Paragraphs 83-84, 102-103, and 36-37 teaches said"reading" and said "comparing". Accordingly, the Examiner has not established a *prima facie* case of obviousness in relation to claim 6.

Based on the preceding argument, Appellants respectfully contend that claim 6 is not unpatentable over Lindeman and Leeds in further view of Liu and is in condition for allowance.

Since claims 7 and 16 depend from claim 3, Appellants contend that claims 7 and 16 are likewise in condition for allowance.

In addition with respect to claim 16, Appellants respectfully contend that Lindeman in view of Leeds does not teach or suggest the feature: "wherein the authentication key is dependent upon only an identity of the originator".

The Examiner argues: "the modified Lindeman, Leeds and Liu system discloses the authentication key is dependent upon only an identity of the originator (see Leeds paragraphs 36 and 37) ."

In response, Appellants maintain that the Examiner has not provided motivation from the prior art for modifying Lindeman with the alleged teaching of Leads with respect to the feature: "wherein the authentication key is dependent upon only an identity of the originator".

In addition, any such modification of Lindeman would destroy the teaching of the CZID of Lindeman, wherein the CZID is essential to Landman's invention. See Landman, Paragraph 29 (" The CZID is **necessary** to authenticate the confirmation message" (emphasis added)). Moreover, the CZID is not dependent upon only an identity of the originator. See Landman, Paragraph 31("The term "CZID" is an MD5 hash of the original sender address, the original destination address, and a secret string. A valid CZID is used to authenticate a message, the source email address, and the destination email address to Spam filter" (emphasis added)). Therefore, the Examiner's suggested modification of Lindeman would destroy Lindeman's invention.

Based on the preceding argument, Appellants respectfully contend that claim 16 is not

unpatentable over Landman and Leeds in further view of Liu .

Claim 10

Since claim 10 depends from claim 9, which Appellants have argued *supra* to not be unpatentable over Landman under 35 U.S.C. §102(e), Appellants maintain that claim 10 is likewise not unpatentable over Landman and Leeds in further view of Liu under 35 U.S.C. §103(a).

In addition with respect to claim 10, Appellants respectfully contend that Landman in view of Leeds does not teach or suggest the feature: "reading a flag from a memory of the recipient at an address that is dependent upon a source identifier that identifies the originator, wherein the flag indicates whether the electronic mail from the originator is expected to include the authentication key; and determining from the flag that had been read from the memory whether the authentication key is expected to be present in the open field of the electronic mail".

The Examiner argues: "As per claim 10, the modified Landman, Leeds, and Liu et al system fails the memory has a flag for determining whether and authentication key is expected.... However, Official Notice is taken that at the time of the invention it would have been obvious to one of ordinary skill in the art to use a flag. Motivation to do so would have been that there are only two possible outcomes."

In response, Appellants contend that the Examiner has not even addressed the specific limitations included in the feature of: "reading a flag from a memory of the recipient at an address that is dependent upon a source identifier that identifies the originator, wherein the flag indicates whether the electronic mail from the originator is expected to include the authentication

key; and determining from the flag that had been read from the memory whether the authentication key is expected to be present in the open field of the electronic mail". Accordingly, the Examiner has not established a *prima facie* case of obviousness in relation to claim 10.

Based on the preceding argument, Appellants respectfully contend that claim 10 is not unpatentable over Landman and Leeds in further view of Liu.

Claim 11

Since claim 11 depends from claim 9, which Appellants have argued *supra* to not be unpatentable over Landman under 35 U.S.C. §102(e), Appellants maintain that claim 11 is likewise not unpatentable over Landman and Leeds in further view of Liu under 35 U.S.C. §103(a).

In addition with respect to claim 11, Appellants respectfully contend that Landman in view of Leeds does not teach or suggest the feature: "reading the stored authentication key from the address at the memory of the recipient, and comparing the authentication key with the stored authentication key that had been read from the address at the memory of the recipient to determine whether the authentication key is associated with the originator".

The Examiner alleges that the preceding feature is disclosed in Landman, Paragraphs 83-84, 102-103, and 36-37.

In response, Appellants maintain that Landman does not disclose said "reading" and furthermore does not disclose said "comparing". The Examiner has not provided analysis to support the Examiner's allegation that Landman, Paragraphs 83-84, 102-103, and 36-37 teaches

said"reading" and said "comparing". Accordingly, the Examiner has not established a *prima facie* case of obviousness in relation to claim 11.

Claims 19

Since claim 19 depends from claim 9, which Appellants have argued *supra* to not be unpatentable over Landman under 35 U.S.C. §102(e), Appellants maintain that claim 19 is likewise not unpatentable over Landman and Leeds in further view of Liu under 35 U.S.C. §103(a).

In addition with respect to claim 19, Appellants respectfully contend that Landman in view of Leeds does not teach or suggest the feature: "wherein the authentication key is dependent upon only an identity of the originator".

The Examiner argues: "the modified Landman, Leeds and Liu system discloses the authentication key is dependent upon only an identity of the originator (see Leeds paragraphs 36 and 37) ."

In response, Appellants maintain that the Examiner has not provided motivation from the prior art for modifying Landman with the alleged teaching of Leads with respect to the feature: "wherein the authentication key is dependent upon only an identity of the originator".

In addition, any such modification of Landman would destroy the teaching of the CZID of Landman, wherein the CZID is essential to Lindeman's invention. See Landman, Paragraph 29 (" The CZID is **necessary** to authenticate the confirmation message" (emphasis added)). Moreover, the CZID is not dependent upon only an identity of the originator. See Landman, Paragraph 31("The term "CZID" is an MD5 hash of the original sender address, the original

destination address, and a secret string. A valid CZID is used to authenticate a message, the source email address, and the destination email address to Spam filter" (emphasis added)). Therefore, the Examiner's suggested modification of Lindeman would destroy Lindeman's invention.

Based on the preceding argument, Appellants respectfully contend that claim 19 is not unpatentable over Landman and Leeds in further view of Liu.

SUMMARY

In summary, Appellants respectfully request reversal of the April 3, 2006 Office Action rejection of claims 3-11 and 13-20.

Respectfully submitted,

Jack P. Friedman

Jack P. Friedman
Attorney For Appellant
Registration No. 44,688

Dated: 09/05/2006

Schmeiser, Olsen & Watts
22 Century Hill Drive, Suite 302
Latham, New York 12110
(518) 220-1850

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.* Examiner: Pyzocha, Michael J.

Serial No.: 09/919,248 Group Art Unit: 2137

Filed: 07/31/2001 DOCKET NO.: **RSW920010143US1**

Title: **AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX A - CLAIMS ON APPEAL

3. An authentication method for electronic mail, comprising the steps of:

storing an authentication key associated with an originator in a memory of the originator;

reading the authentication key from the memory of the originator;

preparing electronic mail for sending from the originator to a recipient, said preparing comprising including the authentication key, that had been read from the memory of the originator, in an open field of the electronic mail; and

sending the electronic mail from the originator to the recipient.

4. The method of claim 3, wherein the electronic mail has a subject line, and the open field of the electronic mail is the subject line.

5. The method of claim 3, wherein the authentication key associated with the originator is

further associated with the recipient.

6. An authentication method for electronic mail, comprising the steps of:

storing an authentication key in a memory of a recipient of the electronic mail at an address that is dependent upon a source identifier that identifies an originator of the electronic mail;

receiving, by the recipient, the electronic mail from the originator;

responsive to receiving the electronic mail, determining whether the authentication key is present in an open field of the electronic mail;

responsive to determining that the authentication key is present, determining whether the authentication key is associated with the originator; and

responsive to determining that the authentication key is not associated with the originator, rejecting the electronic mail,

wherein said determining whether the authentication key is associated with the originator includes: reading the stored authentication key from the address at the memory of the recipient, and comparing the authentication key with the stored authentication key that had been read from the address at the memory of the recipient to determine whether the authentication key is associated with the originator.

7. The method of claim 6, wherein the open field is a subject line of the electronic mail.

8. An authentication method for electronic mail, comprising the steps of:

receiving, by a recipient, electronic mail from an originator;

responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail;

responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present; and

responsive to determining that the authentication key is not expected to be present, accepting the electronic mail.

9. An authentication method for electronic mail, comprising the steps of:

receiving, by a recipient, electronic mail from an originator;

responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail;

responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present;

responsive to determining that the authentication key is not present, rejecting the electronic mail;

responsive to determining that the authentication key is present, determining whether the authentication key is associated with the originator;

responsive to determining that the authentication key is associated with the originator, accepting the electronic mail; and

responsive to determining that the authentication key is not associated with the originator,

rejecting the electronic mail.

10. The method of claim 9, wherein the step of determining whether an authentication key is expected to be present in an open field of the electronic mail includes the steps of:

reading a flag from a memory of the recipient at an address that is dependent upon a source identifier that identifies the originator, wherein the flag indicates whether the electronic mail from the originator is expected to include the authentication key; and

determining from the flag that had been read from the memory whether the authentication key is expected to be present in the open field of the electronic mail.

11. The method of claim 9, wherein the method further comprises storing the authentication key in a memory of the recipient at an address that is dependent upon a source identifier that identifies the originator, wherein the step of determining whether the authentication key is associated with the originator includes the steps of:

reading the stored authentication key from the address at the memory of the recipient; and

comparing the authentication key with the stored authentication key that had been read from the address at the memory of the recipient to determine whether the authentication key is associated with the originator.

13. An authentication method for electronic mail, comprising the steps of:

receiving, by a recipient, the electronic mail from an originator, the electronic mail having been previously prepared for sending from the originator to the recipient;

responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail;

responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present; and

responsive to determining that the authentication key is not present in the open field of the electronic mail, rejecting the electronic mail.

14. An authentication method for electronic mail having a subject line, comprising the steps of:

receiving, by a recipient, the electronic mail from an originator, the electronic mail having been previously prepared for sending from the originator with a source identifier to the recipient with a destination identifier;

responsive to receiving the electronic mail, determining whether an authentication key is expected to be present in an open field of the electronic mail;

responsive to determining that the authentication key is not expected to be present, accepting the electronic mail;

responsive to determining that the authentication key is expected to be present, determining whether the authentication key is present;

responsive to determining that the authentication key is present, determining whether the authentication key is associated with both the originator and the recipient;

responsive to determining that the authentication key is associated with both the originator and the recipient, accepting the electronic mail;

responsive to determining that the authentication key is not associated with both the

originator and the recipient, rejecting the electronic mail; and

responsive to determining that the authentication key is not present, rejecting the electronic mail.

15. The method of claim 3, wherein the authentication key is dependent upon only an identity of the originator.

16. The method of claim 6, wherein the authentication key is dependent upon only an identity of the originator.

17. The method of claim 8, wherein the authentication key is dependent upon only an identity of the originator.

18. The method of claim 9, wherein the authentication key is dependent upon only an identity of the originator.

19. The method of claim 11, wherein the authentication key is dependent upon only an identity of the originator.

20. The method of claim 13, wherein the authentication key is dependent upon only an identity of the originator.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.*

Examiner: Pyzocha, Michael J.

Serial No.: 09/919,248

Group Art Unit: 2137

Filed: 07/31/2001

DOCKET NO.: **RSW920010143US1**

Title: **AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX B - EVIDENCE

There is no evidence entered by the Examiner and relied upon by Appellant in this appeal.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.*

Examiner: Pyzocha, Michael J.

Serial No.: 09/919,248

Group Art Unit: 2137

Filed: 07/31/2001

DOCKET NO.: **RSW920010143US1**

Title: **AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX C - RELATED PROCEEDINGS

There are no proceedings identified in the "Related Appeals and Interferences" section.